

What is claimed is:

1. A data collector comprises:

a device to sample packet traffic, accumulate, and collect statistical information about network flow; and  
a port to link the data collectors over a redundant network to a central control center.

2. A data collector to sample packet traffic, accumulate, and collect statistical information about network flows comprises:

a computing device that executes a computer program product stored on a computer readable medium comprising instructions to cause the computing device to:

perform sampling and statistic collection of data pertaining to network packets; and

parse the information in the sampled packets and maintain the information in a log; and

a port to link the data collectors over a redundant network to a central control center.

3. The data collector of claim 2 wherein the link is a link to a hardened, redundant network.

4. The data collector of claim 3 wherein the hardened redundant network is a telephone network or dedicated leased line.

5. The data collector of claim 2 wherein information collected by the data collector includes source information and destination information.

6. The data collector of claim 5 wherein the data collector collects the information but does not log the sampled packets.

7. The data collector of claim 2 wherein the computer program product in the data collector executes rules to analyze the collected statistics and may if necessary compose a message that raises an alarm to the control center.

8. The data collector of claim 2 wherein the data collector further includes a communication process to respond to queries concerning characteristics of traffic on the network.

9. The data collector of claim 8 wherein the queries originate from the control center and are for information pertaining to statistics collected by the data collector.

10. The data collector of claim 1 wherein the query can be a request to download via the hardened network, a portion of the contents of the log.

11. A method of collecting data from sampled network traffic, pertaining to network traffic flows comprises:  
sampling the network traffic and generating statistics pertaining to the sampled network packets; and  
communicating the generated statistics over a redundant network to a central control center.

12. The method of claim 11 wherein generating further comprises:

monitoring a parameter of traffic flow at multiple levels of granularity.

13. The method of claim 12 wherein monitoring the parameter at multiple levels of granularity is used to to trace the source of an attack.

14. The method of claim 13 wherein monitoring further comprises:

dividing the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter; and

adjusting the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets.

15. The method of claim 11 wherein generating further comprises:

applying multi-level analysis to monitor TCP packet ratios, repressor traffic and statistics based on Layer 3-7 analysis.

16. The method of claim 15 wherein layer 3-7 analysis comprises:

monitoring network traffic for unusual levels of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets.

17. The method of claim 15 wherein layer 3-7 analysis comprises:

monitoring network traffic for IP packets with obviously bad source addresses or ICMP packets with broadcast destination addresses.

18. The method of claim 15 wherein layer 3-7 analysis comprises:

monitoring network traffic for transport control protocol (TCP) or user datagram protocol (UDP) packets addressed to unused ports.

19. The method of claim 15 wherein layer 3-7 analysis comprises:

monitoring network traffic for transmission control protocol (TCP) packets with unusually small window sizes, which can indicate server load, or transmission control protocol (TCP) ACK packets that do not belong to a known connection.

20. The method of claim 15 wherein layer 3-7 analysis comprises:

monitoring network traffic for an indication of a frequency of reload requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection.

21. A computer program product residing on a computer readable medium for controlling a data collector to sample packet traffic, accumulate, and collect statistical information about network flows comprises instructions for causing the data collector to:

perform sampling and statistic collection of data pertaining to network packets;

parse the information in the sampled packets and  
maintain the information in a log; and

communicate statistics generated by the data collector  
to a central control center over a redundant network.